UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/577,756	03/12/2007	Marten E. Van Dijk	US030430US3	8147

24737 7590 02/25/2009

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER
CHAI, LONGBIT

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
02/25/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/577,756	VAN DIJK, MARTEN E.	
	Examiner	Art Unit	
	LONGBIT CHAI	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 March 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5, 7-12 and 14-38* is/are rejected.

7)☒ Claim(s) *6 and 13* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 April 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *4/28/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Priority

1. Applicant's claim for benefit of foreign priority under 35 U.S.C. 119 (a) – (d) is acknowledged.

The application is filed on 2/21/2008 but is a 371 case of PCT/IB04/52235 application filed on 10/28/2004 and has a foreign priority application filed on 10/29/2003.

Claim Objections

2. Claims 1, 9, 16 and 24 are objected to because of the following informalities: a word W' should be replaced with a codeword W'. Appropriate correction(s) is (are) required. Any other claims not addressed are objected by virtue of their dependency should also be corrected.

3. Claim 32 is objected to because of the following informalities: the claim language "a_1… a_N" should be "a_1 … a_n". Appropriate correction(s) is (are) required. Any other claims not addressed are objected by virtue of their dependency should also be corrected.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 1, 9, 24 and 32 are rejected under 35 U.S.C. 101 as not falling within one of the four statutory categories of invention. While the claims recite a series of steps or acts to be performed, a statutory "process" under 35 U.S.C. 101 must (1) be tied to particular machine, or (2) transform underlying subject matter (such as an article or material) to a different state or

thing. See page 10 of In Re Bilski 88 USPQ2d 1385. The instant claims are neither positively tied to a particular machine that accomplishes the claimed method steps nor transform underlying subject matter by imposing meaningful limits or significant steps properly tied to a particular machine, and therefore do not qualify as a statutory process. The recited method claim(s) including steps which are broad enough that the claim could be completely performed mentally, verbally or without a machine nor is any transformation apparent. Any other claims not addressed are rejected by virtue of their dependency.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

1. Claims 1, 9, 16 and 24 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention because, regarding "(d-1)" as recited in the claim, the meaning and range of the notation "d" is not recited in the claim – Examiner respectfully suggests using the claim language – for example, "to create a certain minimum distance d in the codeword to provide to the correspondent with the ability to reconstruct a secret key".

2. Claim 32 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention because, regarding "h(b)" since the claim language "for each symbol b in the set B" may be unclear and confused with a given common numerical number b as an element within an ordered set B – Examiner respectfully suggests to be replaced with "$h(b_j)$ where $j = 1…n$" so that "$h(a_j) = b$" can be clear presented as "$h(a_j) = h(b_j)$", which is also

consistent with the specification (SPEC: page 20, Equation (37)). Any other claims not addressed are objected by virtue of their dependency should also be corrected.

3. Claims 1, 9, 16 and 24 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. The omitted steps are: (a) one of the essential steps missed is the IF condition to generate the key K because, according to the specification, the secret key K can not be always determined and can be determined only under certain / specific condition by the generated codeword W such as "the response from source P 20 to both of first and second correspondents 16 and 18 must be close enough" (SPEC: Page 6, Line 20 – 22) and (b) the secret key K can be determined by the codeword W; however, examiner notes, this subject matter of invention is also rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claims contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains because Examiner notes there are two enablement issues: (i) how to generate a codeword W from the (d-1) parity symbol & the response B and (ii) how to determine the secret key K from the generated codeword W are not disclosed (or presented with an equation) in the specification. One skilled in the art is not enabled as to how to make and use the same claimed invention. For the same reasons, in the lack of this precise description / mechanism / measurement in the specification, the claimed subject matter is not technologically embodied and is merely an abstract idea. Any other claims not addressed are objected by virtue of their dependency should also be corrected.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1 – 5, 9 – 12, 14 are rejected under 35 U.S.C. 102(b) as being anticipated by Maurer (EP 0511420 A1).

As per claim 1 and 9, Maurer teaches a method of secret key agreement between a first (16) and a second (18) correspondent, the method comprising the acts of:

(a) said first correspondent receiving a response A, from a source P (20) (Maurer: Column 7 Line 39 – 47 / Line 14 – 17, Column 11 Line 30 – 35 and Column 18 Line 31 – 34: the string S_A as a response string and a random bit source over three independent channels between the station A and B is considered as a source P to meet the claim language);

(b) said second correspondent receiving a response B from said source P (20) (Maurer: Column 7 Line 39 – 47 / Line 14 – 17, Column 11 Line 30 – 35 and Column 18 Line 31 – 34: the string S_B as a response string and a random bit source over three independent channels between the station B and A is considered as the source P to meet the claim language);

(c) said first correspondent generating (d-1) parity symbols as an output of a codeword W whose input includes said response A and a secret key K selected by said first correspondent (16) (Maurer: Column 9 Line 15 – 17: (N – 1) of parity check bits corresponding to the response strings of (S_A, S_B));

(d) said first correspondent (16) transmitting said (d-1) parity symbols over a public communication channel (22) to said second correspondent (18) (Maurer: Column 14 Line 15 – 18: the string C as (N – 1) of parity check bits is transmitted over the channel); and

(e) said second correspondent (18) generating a word W' whose input includes said (d-1) parity symbols and said response B to determine said secret key K (Maurer: Column 17 Line 21 – 23; a cipher key is generated accordingly).

As per claim 2, Maurer teaches said responses A and B are received by said respective first (16) and second (18) correspondents responsive to a challenge C generated from said respective first (16) and second (18) correspondents (Maurer: Column 18 Line 30 – 35: a request between two station during the communications is considered as a challenge).

As per claim 3, 4, 5, 10, 11 and 12, Maurer teaches said response A is comprised of a sequence of symbols of the form $A=(a_1 \ldots a_n)$ (Maurer: Column 9 Line 13 – 20: any string is indeed constituted with a set of symbols).

As per claim 7 and 14, Maurer teaches the codeword W is a Reed-Solomon codeword (Maurer: Column 20 Line 28: a Reed-Solomon codeword).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 8 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Maurer (EP 0511420 A1), in view of Van (U.S. Patent 2003/0219121).

As per claim 8 and 15, Maurer does not teach the secret key K cannot be determined by someone other than said first and second correspondent (18) if the following inequality is satisfied, $d_H(A, E) >= (d -1)$ is a symbol sequence obtained by an attacker (17) attempting to learn the secret key K, $d_H(A, E)$ is the Hamming distance between the symbol sequences A and E, and d is the minimum distance.

Van teaches the secret key K cannot be determined by someone other than said first and second correspondent (18) if the following inequality is satisfied, $d_H(A, E) >= (d -1)$ is a symbol sequence obtained by an attacker (17) attempting to learn the secret key K, $d_H(A, E)$ is the Hamming distance between the symbol sequences A and E, and d is the minimum distance (Van: Para [0025]: generating a key only if the hamming distance between the first data and the second data is less than a predetermined threshold).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Van within the system of Maurer because (a) Maurer teaches generating a key based upon the Hamming code (Maurer: Column 20 Line 25 – 28) and (b) Van teaches a key generating method by utilizing a Hamming code under the condition if the hamming distance between the first data and the second data is less than a predetermined threshold (Van: Para [0025]).

Allowable Subject Matter

4. Claims 6 and 13 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base

claim and any intervening claims; besides, the base claims 1 and 9 need to be rewritten to overcome the rejection(s) under 35 U.S.C. 112, 2nd / 1st paragraph, set forth in this Office action.

5. Claims 16, 24 and 32 (& its dependent claims) would be allowable if rewritten or amended to overcome the rejection(s) under 35 U.S.C. 112, 2nd / 1st paragraph, set forth in this Office action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LONGBIT CHAI whose telephone number is (571)272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Longbit Chai/

Longbit Chai Ph.D.
Primary Patent Examiner
Art Unit 2431
09/16/2008